TASK ORDER (TO)

47QFCA23F0018

National Background Investigation Services (NBIS) Application and Subsystem Services (NASS) Bridge

in support of:

Defense Counterintelligence and Security Agency (DCSA)
NBIS Program Office

Issued to:
Perspecta Enterprise Solutions LLC

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

March 14, 2023

FEDSIM Project ID 47QFCA22Z0054

C.1 BACKGROUND

The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018, Section 925, (Public Law 115-91) directed the transfer of functions, personnel, and associated resources of the Department of Defense (DoD) Consolidated Adjudications Facility to the Defense Counterintelligence and Security Agency (DCSA), and other organizations as identified by the Secretary of Defense. David L. Norquist, performing the duties of the Deputy Secretary of Defense (DEPSECDEF), issued a memorandum on January 28, 2019, identifying the other organizations to be transferred to DCSA, including Defense Information Systems Agency's (DISA) National Background Investigation Services (NBIS) Program Executive Office (PEO) and subordinate elements; Joint Service Provider (JSP) personnel providing direct support to the DoD Consolidated Adjudications Facility ; and, the portions of Defense Human Resource Activity (DHRA)/Defense Manpower Data Center (DMDC) maintaining and developing the purpose-built Information Technology (IT) systems supporting the Defense Vetting Enterprise. The DEPSECDEF memorandum identified the following vetting systems to transfer from DHRA/DMDC to DCSA: the Defense Information System for Security (DISS); Mirador (the Continuous Evaluation and Records System for Personnel Security); the Secure Web Fingerprint Transmission (SWFT) system, and other systems as mutually agreed upon by DHRA and DCSA. DISS, Mirador, SWFT, and the Defense Central Index of Investigations (DCII), when referred to collectively, are referred to as the “DMDC applications.”

C.1.1 PURPOSE

The DCSA NBIS Program Management Office is seeking experienced professional IT services to support its technology governance and customer development, sustainment, and operational activities, across the Software Development Life Cycles (SDLCs). These services will be performed both onsite DCSA locations and offsite.

C.1.2 AGENCY MISSION

The DCSA is responsible for the development and operation of the NBIS system, which is the Federal enterprise-wide capability that determines the trustworthiness of individuals who work for or support the Government. The capability must facilitate the continuous evaluation of the individual’s credibility for as long as that individual has an association with the Government. DCSA is the security agency in the Government dedicated to protecting America’s trusted workforce and trusted workspaces, real or virtual. DCSA joins two essential missions: Personnel Security and Industrial Security, supported by Counterintelligence and Insider Threat, and Security Training functions. DCSA services over 100 Federal entities, oversees 10,000 cleared companies, and conducts approximately two million background investigations each year.

C.2 SCOPE

The contractor shall provide a full range of IT services, technical and management expertise, and solution-related enabling products in one or more of the functional categories to meet the mission needs of the DCSA for the PSA Applications SWFT, DCII, and DISS. The contractor shall adhere to the performance standards in this contract as well as industry accepted best practices where such does not conflict with the requirements specified while utilizing all proposed innovative solutions and cost savings initiatives. As identified in individual tasks, IT solutions/capabilities will support DCSA on a world-wide basis. The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and any other items or resources to perform this scope of work, including non-personal services necessary to deliver sustainment and operational support activities as defined in this Performance Work Statement (PWS) except for where required by the Government as specified in the PWS.

The contractor will be required to work closely with various divisions within DCSA, and with other agencies to ensure the success of each application. To achieve success the contractor shall have a complete understanding of DCSA's system infrastructure, configurations, tools, and components.

The direct acquisition of weapons or weapons systems on behalf of the DoD is not within scope of this TO. Use of weapons systems, other than as it relates to the analytical and technical services described in Section C, is not within scope of this requirement.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The DCMA systems and applications supported in this environment are as follows. The contractor shall provide support for relevant systems as specified in the tasks of the PWS.

C.3.1 JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

JPAS is officially decommissioned; residual data mining captured by supporting DISS.

C.3.2 SECURE WEB FINGERPRINT TRANSMISSION (SWFT)

The SWFT is a DoD enterprise system for centralized collection and distribution of electronic fingerprints for applicants requiring a background check. SWFT provides the means for collecting biometric data for personnel only once, and then reusing and sharing the data with designated DoD agencies. SWFT eliminates the need for paper-based capture and handling of fingerprints, expedites the background check process by reducing invalid fingerprint submissions, provides end-to-end accountability for sensitive Personally Identifiable Information (PII) data, and implements stringent security standards. The SWFT system consists of two major components:

a. System for web-based enrollment of fingerprints (Web Enroll), which is a licensed Commercial Off-the-Shelf (COTS) product.
b. Store-and-forward system for collection and distribution of electronic fingerprint files (SWFT), which is a Government Off-the-Shelf (GOTS) product.

This integrated system is also known as SWFT Plus Enrollment or SWFT+.

C.3.3 DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII)

DCII is an automated central index that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities. DCII is operated and maintained on behalf of the DoD Components and Office of the Deputy Under Secretary of Defense for Human Intelligence (HUMINT), Counterintelligence and Security. Access to DCII is normally limited to the DoD and other Federal agencies that have adjudicative, investigative and/or counterintelligence missions.

C.3.4 IMPROVED INVESTIGATIVE RECORDS REPOSITORY (iIRR)

The iIRR is in-sourced and operated by Government personnel. No contract support is required.

C.3.5 DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

DISS was developed in response to the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 and the Joint Security and Suitability Reform Team (JRT) focus areas to improve the Federal security and suitability clearance process. This new process was outlined by the JRT in the April 2008 Initial Report on Security and Suitability Process Reform, which provided a framework for an enterprise-wide, end-to-end process supported by appropriate IT systems to make hiring, credentialing, and clearance processes meet IRTPA guidelines on efficiency and timeliness.

The Office of the Under Secretary of Defense for Intelligence (OUSDI) is the functional sponsor and has established and defined the top-level operational requirements for DISS. The DISS solution will support information sharing between various DoD entities, as well as among a number of other Federal agencies. It will be managed and maintained by the DISS Program Management Office (PMO). The DISS PMO will follow guidance of, and escalate issues to, the appropriate DISS Governance Board.

DISS will replace various security clearance and suitability systems, enabling an enterprise solution with consistent standards and reciprocal recognition for all DoD security clearances and suitability/fitness for employment determinations. The DISS program focuses on solutions for three of the reform areas:

a. Validate Need: DISS is working with Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM) to create a federated search capability to support reciprocity and reduce unnecessary duplicate investigation and adjudicative processes.
b. Electronic Adjudication (e-Adjudication): DISS employs technology to apply business rules and render security, suitability, and credentialing adjudication decisions electronically in cases with no actionable issues.
c. Continuous Evaluation: DISS supports the Automated Records Check workflow so records for existing cleared personnel can be analyzed more often to flag potential concerns.

Enhancing these primary areas of the reform security and suitability processes will allow the DISS program to improve timeliness, reciprocity, quality, and cost efficiencies through the design and implementation of a secure, end-to-end IT solution.

a. Case Adjudication Tracking System (CATS): CATS supports the process of rendering an applicant’s eligibility determinations for a security clearance, suitability or fitness for employment, and credentials by providing a framework for assessing an applicant’s trustworthiness and fitness. To date, CATS is successfully implemented at the Army Consolidated Adjudications Facility, Navy Consolidated Adjudications Facility, Washington Headquarter Services (WHS), and Air Force Consolidated Adjudications Facility. These implementations have already achieved substantial improvement in the overall time necessary to adjudicate clearances. CATS will be consolidated into a single, enterprise version within DISS.

b. Joint Verification System (JVS): JVS will provide the functionality for the maintenance and verification of security, suitability, and credentialing eligibility information. JVS will support the concept of a virtual Security Management Office (SMO), providing an access point for Security Officers to manage security information, including subject access levels and eligibility. JVS will be JPAS' replacement.

C.4 OBJECTIVE

Services provided under this TO shall include Project Management and SDLC requirements. The specific depth and breadth of the activities will vary over the implementation of the project, and include requirements definition, functional and technical specifications, design, project planning, development, testing, and implementation. With the pace of change, it is impossible to anticipate how IT requirements and programs will evolve over the life of the contracts. These services represent a broad set of contemplated work requirements and should not be construed as the only activities to be to be performed on this TO.

C.5 TASKS

The contractor shall provide sustainment and operational support for all identified Personnel Security/Assurance (PSA) Applications. The contractor shall also provide DISS development support, ensure data accuracy, conducted testing, and perform Configuration Management (CM) activities.

The following task areas are detailed below:

a. Task 1 – Program Management
b. Task 2 – Sustainment and Operational Support of PSA Applications of Subsystems
c. Task 3 – Customer, Data, and Field Support
d. Task 4 – Testing Support
e. Task 5 – Configuration Management (CM) Support
f. Task 6 – Information Assurance (IA) Support
g. Task 7 – DISS Development Support (CATS and JVS)
h. Task 8 – PSA Systems Optional Support (T&M)

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide management and oversight of all activities performed by contractor personnel, including subcontractors, to meet the requirements identified in this PWS.
The contractor shall provide program management support under this TO utilizing industry best project management practices (i.e., Project Management Body of Knowledge (PMBOK®) Guide), which include all the tasks required to initiate, plan, manage, control, report, and close-out this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors/teaming partners, to satisfy the requirements identified in this PWS.

The contractor shall document their approach in a Project Management Plan (PMP) **(Section F, Deliverable 06)**. The initial draft PMP shall be submitted in accordance with the TO Schedule and Milestones in Section F.3. The PMP shall describe the contractor's management approach, operating procedures, support priorities, service levels, and estimated staffing. The PMP shall include an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations. The PMP shall show milestones and tasks for short term and long-term projects. The PMP shall, at a minimum, address:

a. Process management and control (i.e., monitoring mechanisms, program metrics).
b. Personnel management to include coverage and organizational structure.
c. Financial management to include cost containment and cost forecasting.
d. Technical Effectiveness to include routine Operations and Maintenance (O&M) and implementation and integration of new hardware and software, and technical refresh procedures.
e. Operational effectiveness to include system administration, account management, implementation of new hardware and software, and technical refresh procedures.
f. Establishment of task support in relation to incrementally provided funding in accordance with customer established task priorities.

The contractor shall provide the Government with a draft PMP, on which the Government will make comments. The final PMP shall incorporate Government comments. The contractor shall keep the PMP up to date in accordance with the Deliverables table.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR SERVICE CONTRACT REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for DCMA. The contractor shall completely fill in all required data fields using the following web address: http://www.sam.gov.

Reporting inputs will be for the labor executed during the period of performance during each Government FY, which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported No Later Than (NLT) October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.sam.gov.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (**Section F, Deliverable 01**). The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the contractor's Key Personnel, the DCSA Technical Point of Contact (TPOC), other relevant Government personnel, the FEDSIM CO, and the FEDSIM COR.

At least three days prior to the Project Kick-Off Meeting, the contractor shall provide a Project Kick-Off Meeting Agenda (**Section F, Deliverable 02**) for review and approval by the FEDSIM COR and the DCSA TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (e.g., roles and responsibilities and lines of communication between contractor and Government).
c. Project Staffing Plan and status.

d. Transition-In Plan (**Section F, Deliverable 08**) and discussion.
e. Security discussion and requirements (e.g., building access, badges, Common Access Cards (CACs)).
f. Financial reporting and invoicing requirements.
g. Baseline Quality Management Plan (QMP) (**Section F, Deliverable 11**).

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting, and the contractor shall provide copies of the presentation for all present.

The contractor shall draft and provide a Project Kick-Off Meeting Minutes Report (**Section F, Deliverable 03**) documenting the Project Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PREPARE SENIOR MANAGEMENT REVIEW (SMR) REPORT

The contractor shall develop and provide SMR Reports (**Section F, Deliverable 10**) using the template provided in Section J, Attachment U. An SMR report shall be submitted NLT the 15th of each month. The SMR shall include the following:

a. Activities during the reporting period, by task (include ongoing activities, new activities, activities completed, and progress to date on all above-mentioned activities). Each section shall start with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Activities anticipated during the next reporting period.

C.5.1.4 SUBTASK 4 – CONVENE BI-MONTHLY STATUS MEETINGS

The contractor shall convene bi-monthly status meetings (**Section F, Deliverable 04**). The purpose of this meeting is for coordination and information sharing with DCSA and other Government stakeholders. This meeting shall contain all initiative statuses (e.g., status, timelines, risks, issues), open DCSA/stakeholder's ad hoc reports, recommendations, and any other necessary information that the Government needs to be aware of.

The deliverable (electronic and hard copy) shall be the following:

a. Provide meeting minutes (**Section F, Deliverable 05**) to the FEDSIM COR and DCSA TPOC within five workdays.

C.5.1.5 SUBTASK 5 – CONVENE IN-PROGRESS REVIEW (IPR)

In addition to the specific deliverables and associated reviews listed, the contractor shall schedule, organize, and present IPRs (**Section F, Deliverable 12**), no less than bi-annually, during the period of performance of this TO. The method of presentation shall be in the contractor's PMP. The objectives of these reviews are to track progress of the project, present ideas for improvement, and identify and resolve issues. The contractor shall coordinate the requirements of the IPR with the DCSA TPOC and FEDSIM COR.

C.5.1.6 SUBTASK 6 – PREPARE PROBLEM NOTIFICATION REPORT (PNR)

The contractor PM shall notify the DCSA TPOC and FEDSIM COR of any problems or potential problems affecting performance. Verbal reports of problems shall be followed up with written PNRs (**Section F, Deliverable 13**) within ten calendar days.

C.5.1.7 SUBTASK 7 – PROVIDE QUALITY MANAGEMENT

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified (**Section F, Deliverable 11**). The contractor's QMP shall describe the application of the appropriate methodology (e.g., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

C.5.1.8 SUBTASK 8 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (**Section F, Deliverable 07**) when the request for travel is submitted. The contractor shall keep a summary of all Long-Distance Travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, Trip Reports shall be prepared with the information provided in Section J, Attachment F.

C.5.1.9 SUBTASK 9 – TRANSITION-IN

The contractor shall provide a Transition-In Plan (**Section F, Deliverable 08**) as required in Section F. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan NLT ten calendar days after award, and all transition activities shall be completed 60 calendar days after Program Start (PS).

C.5.1.10 SUBTASK 10 – TRANSITION-OUT

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within six months of PS (**Section F, Deliverable 09**). The contractor shall review and update the Transition-Out Plan in accordance with the specifications in Sections E and F.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. POCs.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.

e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel roles and responsibilities.
g. Schedules and milestones.
h. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.2 TASK 2 – SUSTAINMENT AND OPERATIONAL SUPPORT OF PSA APPLICATIONS AND SUBSYSTEMS

The contractor shall provide ongoing sustainment and operational support for the PSA applications and subsystems within the production, pre-production, Continuity of Operations Plan (COOP), development, and test environments and ensuring all aspects of the applications, including any reports, continue to function. The contractor support shall include application and Operating System (OS) level and below (IAVM patch testing and support) for all systems. DCII environments will transition to DCSA Cloud infrastructure. This effort will require support for each of the technologies used for the applications.

a. For DISS: The development environment shall be maintained in the contractor location.
b. For SWFT and DCII: The contractor shall provide expert services and support to NBIS PMO and Data Center personnel to complete infrastructure transitions. SWFT production is located at the Defense Enterprise Computing Center (DECC) in Columbus, Ohio and PPRODD, COOP, Test, and Development will be transitioned to DECC Ogden, UT. DCII instances will be migrated to DCSA NBIS Amazon Web Services (AWS) Cloud West. The contractor shall support the NBIS PMO and business partners to complete the infrastructure transition by adhering to methods, processes, and systems to include accreditation, SNAP, CSSP, Cloud Permission to Connect, HBSS, ACAS, Nagios, Privileged Access Manager, Sitescope, cut over, end-to-end testing and others. The contractor shall provide support for all data sources for the systems from planning, implementation, and testing.

The contractor shall detect all outage/issue/problems that adversely affect the performance and/or vulnerability of the systems and work with DCSA Systems to assist to resolve the outage/issue/problem, and notify the Government/stakeholders, as defined by DCSA, as soon as possible. The contractor shall follow all DCSA NBIS operational processes and procedures for sustainment and maintenance.

a. For DISS and SWFT: The contractor shall have a proactive approach for utilizing automated system-monitoring techniques to identifying recurring problems, reporting to the Government those problems, and recommending solutions to mitigate recurring problems of the same nature. The contractor shall resolve all outage/issue/problems and work with systems to resolve all outage/issue/problems.

The contractor shall provide support by assisting in identifying and resolving application system problems and/or vulnerabilities. This includes recommendations, consultations, coordination, evaluation, testing, and deployment to resolve.

a. For SWFT, and DISS: The contractor shall identify and resolve application system problems and/or vulnerabilities.

The contractor shall provide database administration services that shall perform modifications to the PSA applications while maintaining continuity of the data to include performing schema changes and conversion of the production database during application upgrades and new version releases.

a. For DISS and SWFT: The contractor shall provide administration services from the application to OS.

The contractor shall provide support, maintain, and keep the test, development, and pre-production PSA applications consistent with current application upgrades and new version releases, while providing database refreshment of all database instances. The contractor shall ensure that all data used in these environments follow DCSA's PII Policies. Data will need to be refreshed at the request of the Program Manager.

a. For the DISS application, the contractor shall manage the software development enclave in a contractor-provided location that meets minimum standards for confidentiality, integrity, and availability.
    1. The software development enclave shall be built in such a way that it will meet with the National Institute Of Standards And Technology (NIST) Special Publication 800-171, Revision 2 (https://doi.org/10.6028/NIST.SP.800-171r2) controls for Federal systems. (If there is a newer version published by the NIST the contractor will be responsible for updating within the first 90 days of the enclave's use by the contractor.) Deviations from the NIST SP800-171 guideline will be reviewed by the COR, DISS Systems Owner and DCSA Capability Analysis and Measurement Organization (CAMO) prior to placing the DISS software in the enclave.
    2. Compliance will be assured through annual reviews by the COR, DISS System Owner (through the NBIS cybersecurity team) and DCSA CAMO team for final review. Open risks will be assessed and referred for action.
    3. The contractor shall utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. The reports shall be available for review as requested by the DISS System Owner.
    4. Network, security and communication path designs shall be available for Government review prior to enablement and at any time as requested but no less than annually.
    5. The contractor will maintain the enclave within best practices for known vulnerability management. Scans will be available to the Government for review on a monthly basis, at least.
    6. Code scanning will be provided by the contractor on a regular basis and/or new versions or updates to the DISS software are presented to the PPROD and PROD enclaves. The code scans should be completed with an automated up to date code

scanning tool. The reports shall be provided and approved prior to installing the software in the Government enclaves (i.e., DISA datacenters enclaves).

b. For SWFT, and DISS: The contractor shall support, maintain, and keep the test, development, and pre-production PSA environment consistent with current application upgrades and new version releases, while providing data refresh on all database instances.
c. For DISS: The contractor shall build out the necessary environment(s) to allow for the PII to be removed and to be used to replace the PII environments that are currently being used by the data team. Some work will be dependent on another contractor. The contractor may need to work with another prime contractor for access to the necessary environment.
d. For DISS: The contractor shall provide Splunk application administration on the operating environment at the DISA DoD Data Center. Splunk will be required for DISS to audit user actions on subject records. The current Splunk application at the DISA DoD Data Center utilizes Linux software. The contractor will be responsible for providing Splunk application maintenance (e.g., patching and security updates) via remote access.
e. For DISS: The contractor shall provide and sustain DISS test record generator tool for use in the development and test environments.

The contractor shall assist in failover planning, testing, and execution at least once a year and during any major outage where when the Government deemed failover necessary.

a. For SWFT, and DISS: The contractor shall conduct failover planning, testing, and execution at least once a year and during any major outage when the Government deemed failover necessary.

The contractor shall modify the applications in accordance with Change Requests and Problem Reports approved by the DCSA TPOC.

The contractor shall collaborate with PSA system's partnering stakeholders (e.g., OPM, Diplomatic Security Service (DSS), armed services, accessions) to maintain fully functional interfaces, process data; resolve data and/or technical issues; and/or update the interfaces when needed. This includes decommissioning of interfaces when no longer needed and updating the interfaces as the partnering agency transition over to new country codes, if applicable. The contractor shall provide support for tech refreshes and enhancement to maintain security and functionality of the systems. Additionally, the contractor shall support partnering agencies to move the application to various SDLC environments (Development, Test, PPROD, PROD) and support the migration and transition to data center and cloud infrastructures.

The contractor shall ensure that quality assurance requirements are enforced for all aspects of the software revision process. This includes collecting and analyzing quality metrics, performing detailed reviews, walkthroughs, requirement traceability analyses, defined verification and validation processes that occur during the course of software maintenance to ensure that requirements are traceable, consistent, complete, and successfully tested. The contractor shall ensure the software correctly reflects the documented requirements which include conducting, reporting on, and/or participating in formal reviews, informal reviews, inspections, peer reviews, tests, and evaluations to ensure the code meets operational and security requirements and does not negatively impact performance of the system.

The contractor shall provide the following deliverables for the Sustainment and Operational Support of PSA Applications and Subsystems Task:

a. Software Requirements Specification (**Section F, Deliverable 14**)
b. Release Notes (**Section F, Deliverable 15**)
c. User Guides (**Section F, Deliverable 16**)
d. Interface Control Document (ICD) (**Section F, Deliverable 17**)
e. Administration Guide for DISS (**Section F, Deliverable 18**)
f. COOP for DISS (**Section F, Deliverable 19**)

C.5.3 TASK 3 – CUSTOMER, DATA, AND FIELD SUPPORT

The contractor shall maintain and ensure data accuracy and data integrity. The contractor shall analyze and resolve data errors/issues/problems. If any data integrity/error/issue with a record is identified, the record shall be updated/corrected within 14 business days or within timeline specified/agreed upon by the PSA Application PM, and the resolution will be communicated to the Government, stakeholder, customer, and/or interface. If the source of the problem originates from an interface, communication to the data source/interface shall be made within 48 hours of discovery to include identification and recommendation for problem resolution. This coordination with external interface owners/customers for data correction also includes periodic and timely follow-ups until the data issue is resolved.

For this task, the contractor shall:

a. Provide a data quality assurance team to ensure data conforms to data standards. This task may include performing quality control checks to DISS data, verifying scripts, correcting data and ensuring data is meeting standards set by the Government to ensure that DISS data will not only meet data quality standards but also be able to be migrated.
b. Add, create, modify, or delete super users/non-DOD/special circumstances user accounts or settings within three business days of notification unless immediate add/modification/removal is needed.
c. Create and provide customized reports or data extracts based on DCSA or stakeholder's requirements. Reports or data extracts shall be provided within seven business days from receiving the Government's request or within timeline specified by the PSA Application PM.
d. Review, evaluate, advise, provide answers and/or guidance on products or deliverables relating to the PSA Applications to the Government, Stakeholders, Call Center, and customers.

For SWFT: The contractor shall act as the POC between the SWFT user community and Government to coordinate and manage day to day SWFT activities. This function is generally known in the SWFT user community as the SWFT Coordinator, and includes the following responsibilities:

a. Monitor and maintain the SWFT mailbox ensuring that all requests, questions, issues and other communications are addressed within two business days.
b. Manage and coordinate the registration and approval process for fingerprint capture devices with DCSA, OPM or other entities.

c. Coordinate with the SWFT Administrators timely release of electronic fingerprints to their requested destinations.
d. Coordinate with the Call Center/Help Desk and the SWFT Administrators the resolution of issues related to the SWFT application.
e. Produce and maintain program documentation such as: weekly activity reports, system metrics, SWFT registration documents, and SWFT Frequently Asked Questions (FAQs)
f. Monitor, analyze, and report on processes and procedures related to the use of the SWFT system, fingerprint submissions, fingerprint submission site and fingerprint capture device registration, and make recommendations for improvement and enhancement.

For SWFT: The contractor shall act as the POC between the online fingerprint enrollment user community and DCSA to manage and coordinate day to day activities. This function includes the following responsibilities:

a. Create and manage online enrollment system user accounts.
b. Create, manage and assign the enrollment user groups, sub-groups, and location profiles.
c. Respond to client communications and ensure that all requests, questions, issues and other communications are addressed within two business days.
d. Coordinate with the SWFT Coordinator and Administrator timely release of electronic fingerprints.
e. Coordinate timely resolution of issues related to online fingerprint enrollment with the Help Desk, SWFT Administrators and SWFT application technical support.
f. Produce and maintain program documentation such as: weekly activity reports, system metrics, and FAQs specific to online fingerprint enrollment.
g. Monitor and analyze processes and procedures related to online fingerprint enrollment subsystem usage, fingerprint submission traffic, fingerprint enrollment site, and fingerprint capture device registration, and make recommendations for improvement and enhancement.

For DISS: The contractor shall act as the operational POC between the DISS user communities; monitor and maintain the DISS mailbox(es) ensuring that all requests, questions, issues, and other communications are addressed within two business days; coordinate with the Call Center/Help Desk and the System Administrators for the resolution of issues related to the DISS applications; produce and maintain program documentation such as: weekly activity reports, system metrics, and standard operating procedure(s); monitor, analyze and report on processes and procedures related to the use of DISS application(s), and make recommendations for improvement and enhancement.

For DISS: DISS shall be able to receive data from CE in order to place a new investigation on a subject's record. This will include a CE Alert Flag to identify if a CE alert is on a subject's record as well as a CE investigation history start date and end date on a subject's record. There may be multiple CE investigations, dependent on DoD affiliation. There also may be multiple CE alert flags at various times.

The contractor shall provide the following deliverable for the Customer, Data, and Field Support Task:

a. SWFT Quarterly Newsletter (**Section F, Deliverable 20**)

C.5.4 TASK 4 – TESTING SUPPORT

The contractor shall develop and conduct thorough testing in the development and test environments to ensure optimum performance is maintained to include functional testing of interfaces and application changes, as defined in the Functional Test Plan, prior to releasing the software and/or IA patches for testing in the Government's pre-production environment.

a. For SWFT and DISS: Upon completion of the contractor's initial testing and quality assurance testing, all software coding shall be tested in the Government's pre-production environment to ensure proper validation of enterprise systems and applications prior to deployment into the production environment.
b. For DCII: The contractor shall conduct functional testing prior to releasing the software and or IA patches to the production environment.

The contractor shall ensure all errors identified during the tests, to include tests in the Government's pre-production environment are resolved. Once testing has been accepted by the Government, the modifications can be deployed to production.

The contractor shall provide the following deliverable for the Testing Support Task:

a. Test Management Plan (TMP) for DCII, SWFT, and DISS (**Section F, Deliverable 21**)

C.5.5 TASK 5 – CONFIGURATION MANAGEMENT (CM) SUPPORT

The contractor shall perform the CM activities of configuration status accounting, configuration baseline management, creating, and maintaining a CM library system to control the release of products, manage their history, administering a change management procedure, and tool to track all Change Requests or Problem Requests to the baseline as well as all issues.

The contractor shall perform the accepted and practiced DCSA CM processes in conjunction with internal and external procedures, plans, and policies of DCSA to include informing, coordinating, providing and documenting all baseline system documentation, modifications to existing and developing system(s) through the DCSA CM group. Baseline system documentation includes system designs, build procedures, requirements documents test procedures, problem reports, software code, and system knowledge base.

The contractor shall provide the following deliverable for the CM Support Task:

a. CM Plan (**Section F, Deliverable 22**)

C.5.6 TASK 6 – INFORMATION ASSURANCE (IA) SUPPORT

NOTE: For PSA Applications running in standard DCSA infrastructure, the scope of this task will be generally limited to application-level support. For SWFT, and DISS, the scope of support is from application to OS.

The contractor shall perform all work within the scope of this contract in strict compliance with all applicable DoD Security Regulations and DoD IA Regulations, United States Cyber Command (USCYBERCOM) Orders, Federal Information Security Management Act (FISMA) and DCSA Security policies to include: maintaining the Trusted Facilities Manual and Security Features Users' Guide required by DoD, monthly IA Security Vulnerability Reports, participating in the Certification and Accreditation (C&A) process, using protective tools such as Security Technical Implantation Guide (STIG), Security Readiness Reviews (SRRs) or checklist on a reoccurring basis using the appropriate tool (or other tool as defined by the Government), providing and implementing the necessary IA/Computer Network Defense (CND).

The contractor shall create and adhere to procedures & guidelines which are created to comply with DoD and DCSA security policies. The contractor shall ensure that all data leaving DCSA systems in transit or at rest be protected according to Department of Defense Instruction (DODI) 8500.2. Specific policies are listed as DODD 8500.1; DODI 8500.2; DODD 8570.01-M; DODD-O-8530.1; DODD-O-8530.2; and DoD 8510.10. These policies are available at http://www.dtic.mil/whs/directives/corres/ins1.html.

The contractor shall take immediate action to assess the impact of each vulnerability, develop patching plans, provide First Report requirement, create the necessary Plan of Action and Milestones (POA&M), and test patches to ensure no negative impact. Testing shall be conducted to ensure IAVM actions will not impair system operations.

a. For SWFT and DISS: The contractor shall assess, review, test and coordinate weekly IAVMs for OS and Database components with data center admin personnel. The contractor shall patch all application software and server components accordingly while following DCSA's IA policies and regulations. IAVM compliance will be ensured through 1) the normal C&A process, and 2) monthly scanning of the systems using tools used by DCSA. The results of these scans will be sent to the Information Assurance Officer (IAO), to be identified post award. This task does not include SWFT.

The contractor shall support obtaining accreditation via certification testing of its respective element(s). This task will consist of process, analysis, coordination, security certification test, self-evaluation, conducting system security assessments, and security documentation support, assisting the Government in the implementation of C&A.

The contractor shall ensure the Information Assurance Manager (IAM) and IAO are informed on system security matters; address specific security issues and obtain guidance.

a. For DISS: The contractor shall provide any necessary documentation (e.g., C&A reports, Monthly Vulnerability Reports, First Reports, POA&Ms) to DCSA's IAO.

The contractor shall provide the following deliverables for the IA Support task:

a. Monthly Vulnerability Analysis Report for DISS (**Section F, Deliverable 23**).
b. IA Report for DISS (**Section F, Deliverable 24**).

C.5.7 TASK 7 – DISS DEVELOPMENT SUPPORT

The contractor shall continue the development of the full set of sub-applications and services to include development of data delivery components implementing the functional and technical requirements, architecture, and all data and security services.

The contractor shall ensure proper authentication and authorization of a user, based on their individual role and level, are allowed proper access by using subject and SMO data services to read data. Authentication will utilize all DOD-approved Public Keys and will utilize existing DCSA application security and operator provisioning services.

DISS application development assumptions:

a. Agile development strategy to meet the emerging requirements of the user communities.

b. Quarterly deployment of major code releases for each DISS component with minor releases as needed to address defects, mandated updates, etc. (Total: eight annual releases).
c. Application updates due to policy changes will be prioritized for release within 60 days unless otherwise specified by the Government.
d. Application, workflow, and data delivery services changes related to the transition of DISS capabilities and populations into NBIS will be prioritized for release within 60 days unless otherwise specified by the Government.

In support of this task, the contractor shall:

a. Maintain subject-related data services to create, read, update, and search for subject information.
b. Maintain SMO data services to create, update, and deactivate SMOs, and manage SMO-subject relationship information and tasks.
c. Maintain eligibility data services to create, read, update, and remove eligibility information for subjects.
d. Maintain foreign relationship and foreign trip data services to create, read, update and delete foreign relationship and foreign trip information for subjects.
e. Maintain access data services to grant, remove, suspend, and reinstate access for subjects to classified data.
f. Maintain visit data services to create, validate, access, and modify visit information for a subject's visit to a facility to discuss/access classified information.
g. Develop incident data services to create, update and close incidents that would impact a subject's eligibility and/or access to classified information.
h. Develop notification/message data services, including support for continuous evaluation to notify users and SMOs of various activities during the operation of the system.
i. Ensure, for all services that are developed, full integration with the DCSA Application Programming Interfaces (APIs), DCSA's application security and operator provisioning services, ensuring that proper transactions are maintained at all times, and shall rollback any uncommitted transactions.
j. Ensure that authorized users have the ability to access all functionality of the application to include add, update/modify, delete based upon their user role and level.
k. Provide systems engineering support to include the development of software development lifecycle documents and participate in technical reviews of the documents.
l. Maintain the Extract, Transform, and Load (ETL) capability.
m. Develop referential integrity rules to be applied to screened data to ensure that proper relational database design integrity is applied throughout the destination database.

The contractor shall provide the following deliverables for the DISS Development Support Task:

a. Functional Test Guide (**Section F, Deliverable 25**).
b. Source Code and Configuration Files (**Section F, Deliverable 26**).
c. Executable Software Libraries (**Section F, Deliverable 27**).
d. High Level Design (HLD)/Low Level Design (LLD) Document (**Section F, Deliverable 28**).

e. As-Is Documentation (**Section F, Deliverable 29**).
f. Updates to Technical Architecture Designs and Components (**Section F, Deliverable 30**).
g. Current State Application Modeling (**Section F, Deliverable 31**).
h. Architecture Analysis (**Section F, Deliverable 32**).
i. Plans, Artifacts, and Design Configurations in DCSA and NBIS infrastructure (**Section F, Deliverable 33**).
j. Integration Recommendations for Cloud Computing (**Section F, Deliverable 34**).
k. Gap Analysis (**Section F, Deliverable 35**).
l. Data Management Plans (**Section F, Deliverable 36**).
m. Data Architecture Plans (**Section F, Deliverable 37**).
n. Database Design and Modeling (**Section F, Deliverable 38**).
o. Analyses of Current Application Inventory (**Section F, Deliverable 39**).
p. Function and Capability Crosswalk (**Section F, Deliverable 40**).
q. Technology Assessment Evaluation (**Section F, Deliverable 41**).
r. Strategies for Performance Load/Stress Testing (**Section F, Deliverable 42**).
s. Develop Capacity of the Current and Future Growth of Application Infrastructure (**Section F, Deliverable 43**).
t. Strategies for CI and CD (**Section F, Deliverable 44**).

C.5.8 TASK 8 – STANDARDIZATION AND INTEGRATION SUPPORT

As requested by the Government, the contractor shall provide analysis and modifications necessary to support the standardization, integration, and enhancement of DCSA applications and subsystems. This may include enhancements to applications, design changes to applications, standardization of applications, development of shared components, integration between applications, testing of new application requirements, and modifications due to policy changes.

C.5.8.1 SUBTASK 1 – INTEGRATION SUPPORT

DISS and SWFT are DoD capabilities identified for integration into the NBIS designated to replace the OPM information technology in support of an end-to-end Federalized solution for national security, suitability, and Personal Identity Verification (PIV) credentialing eligibility determinations. DCSA and NBIS will leverage agile best practices for software development to provide the iterative products and services that will require rapid adjustment to meet integration goals as system capabilities are delivered while allowing the continued use of these production systems.

The contractor shall provide the following services in support of DISS, SWFT, and other applicable DCSA/NBIS system integration as directed by the Government:

a. Integration of DISS, SWFT, and other applicable DCSA systems into a common NBIS Data Repository that will be shared with other NBIS systems. This will require modifications to the applications as well as the underlying architecture. The contractor is not expected to perform migration services.
b. Standardization and rationalization of the DISS, SWFT, and other applicable DCSA/NBIS systems as appropriate to improve integration.

c. Integration with other DCSA applications (e.g., FTS (Fingerprint Transmission System), e-App (replacement for OPM's e-QIP, and a Case Management application).
d. Increase of security controls and postures of DISS, SWFT, and other applicable DCSA systems from the infrastructure, architecture, data, and application perspectives.
e. Implementation of the DCSA applications into different NBIS environments to include but not limited to Development, Test, Production, and Disaster Recovery.
f. Delivery of interfaces with the DCSA system components to support transitional capabilities (e.g., eQIP, Mirador).
g. Development of interfaces with new NBIS system components in parallel development cycles.
h. Modification of additional workflows to meet Government requirements.
i. Integration of capabilities from existing OPM systems components (e.g., CVS).

The contractor shall provide the following deliverable in support of this subtask:

a. Capability Integration Status Report as requested by the Government (**Section F, Deliverable 47**).

C.5.8.2 SUBTASK 2 – ANALYSIS SUPPORT

In order to move applications from SWFT, DCII, and DISS to the Defense Information Systems Agency (DISA) and/or Defense Enterprise Computing Centers (DECCs), the Government requires the contractor to define and document the current as-is and to-be architecture for PSA environments.

The contractor shall provide the following current state Application Modeling Support:

a. Create current state application modeling in coordination with Architecture Review Board (ARB) and other entities as part of the modeling efforts, integration with DCSA and/or National Background Investigation System (NBIS) service management processes, configuration management and change impact analysis and reporting on application deployment.
b. Document and maintain current state application inventory, deployment details and information to enable configuration management. Documentation shall be created using DCSA and/or NBIS standardized Enterprise Architecture Repository, include full system and asset inventory, and provide reporting capabilities at the request of the Government.
c. Support the Government Architecture Program Manager responsible for the definition, documentation, and execution of the DCSA and/or NBIS EA business structure and the Software Development Life Cycle (SDLC) process, its policies, processes and standards.
d. Architectural and technical oversight engagement activities including long- and short-term participation with application development and IT infrastructure operations teams providing full SDLC support, tool support, mentoring, and architectural design and implementation support with consideration for application performance.
e. Assist the DCSA and/or NBIS CIO with the planning, design, configuration, and establishment of applications in the DCSA and/or NBIS infrastructure and architecture.
f. Incorporate and/or revise technical architecture components, to include modifications necessary for NBIS effort.

g. Assist the DCSA and/or NBIS CIO with the planning, design, configuration, and transition support into the NBIS infrastructure and architecture. Support will require coordination and collaboration with other Federal Agencies (e.g., SPAWAR) that are pursuing integration into the NBIS environment. Provide detailed artifacts needed for full transition and integration into Cloud Computing and/or alternate environments.
h. Provide Test Development environments as part of the NBIS effort.

The contractor shall provide the following Architecture Sustainment Support:

a. Research new techniques and standards from the government and industry to implement best practices, refine knowledge, and provide guidance through assisting or providing formal and informal knowledge transfer to DCSA and/or NBIS staff.
b. Support Architecture maturation efforts by assisting in the identification and documentation of recommendations for process improvements, new process adoption efforts, and tool adoption and support. This support includes, but is not limited to, tasks such as process mapping, point papers, process research and reengineering, and implementation support, for Government approval and implementation.
c. Provide business architecture documentation support that provides information for decision making for the Government regarding effective IT investments supporting business requirements. These business requirements are linked to the DCSA and/or NBIS Division level Strategic Plans, and provide maximum business value to customers, both internal and external.
d. Work with divisional groups to complete business and IT architecture planning.
e. Assess business drivers and IT capability; perform, document, and deliver a gap analysis within 30 days of task order modification award.
f. Develop IT vision and business/IT alignment statements for Government review and approval.
g. Establish and document the alignment of business, functional, and IT goals and objectives.
h. Conduct analysis support to ensure requirements compliance, identify problems, correctly attribute them to automated processes and/or submission data, and develop solutions.
i. Respond to ad hoc research requests from management to include: performing special studies, conducting data research and responding to inquiries for customers.
j. Develop and maintain architectural design documents and present them to the Government for review and approval.
k. Develop and maintain comprehensive Data Management Programs that include key components such as data architecture; data dictionary; data models; data and metadata repositories; data stewardship; data quality; data acquisition; data usage; and data retention.
l. Work with Divisional groups to support the development of data architecture planning and implementation initiatives.
m. Determine project schema requirements and establish guidance on enterprise modeling standards as they apply to the production and test databases.
n. Participate in logical database design and modeling. Collaborate with the data architects and the enterprise data modeler team to review and publish application logical data models.

o. Make recommendations for incorporating DCSA and/or NBIS approved technical architecture components into applications using DCSA approved software frameworks (e.g., Java Enterprise Edition (J2EE), Common Update Framework (CUF) and Application Security).

p. Conduct application architecture initiatives, such as identifying and classifying application components according to the specific business and performance objectives they support and the technologies they employ.

q. Document and perform analyses of the current application inventory and provide detailed application architecture guidelines to improve both business and technology processes and applications in the interest of integration and cost containment. Application analysis may require research of Gartner Magic Quadrant, interoperability capability, performance and scalability, reliability and availability, application lifecycle stage, and technological risks.

r. Provide support to identify and recommend application delivery; what technologies should be used to deliver them, and how the applications should be designed, deployed, and integrated in the most effective and flexible way.

s. Recommend updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments with impact analysis for Government review and approval.

t. Support requirements gathering and high-level design for IT application development.

u. Support development of business requirements documents.

v. Assess and document the alignment of applications/services to Agency programs.

w. Work with Divisional groups to support application architecture planning, implementation, and maintenance.

x. Provide support in assessing performance of applications in producing business value and return on investment.

y. Work with Divisional groups to support IT architecture/infrastructure planning, implementation, and maintenance.

z. Provide technology assessment feedback as required.

aa. Identify and document hardware and software technology refresh recommendations.

bb. Evaluate opportunities for delivery of common capabilities for describing, organizing, integrating, sharing, and governing information assets.

cc. Prepare application and infrastructure for migration to Cloud computing with various environments (Production, Test, Development, Pre-Production).

dd. Provide support in assessing performance of infrastructure in producing business value and return on investment. Analyze and recommend the gap requirements on current DISA Service Level Agreement (SLA).

ee. Input all modeling artifacts into the Government defined tool and/or system.

ff. Develop strategies to support end-to-end infrastructure metrics and Key Performance Indicator (KPI) and develop performance load/stress testing strategies.

gg. Assess performance metrics and define, plan, and monitor the capacity of the current and future growth of application infrastructure.

hh. Develop strategies on Continuous Integration (CI) and Continuous Deployment (CD) which involve an automated build system for quicker release and roll back of application.

ii. Document and perform analyses of the current and all future internal and external application interfaces and provide detailed application architecture guidelines to improve both business and technology processes and applications in the interest of integration and cost containment.

The contractor shall provide the following deliverable in support of this subtask:

a. 'To-Be' Report (**Section F, Deliverable 48**) including recommendations as requested by the Government.

b. Initial Data Management Plan (**Section F, Deliverable 49**) is due 45 days after TO award; the plan shall be updated as required by the Government.

c. Build and submit a Function and Capability Crosswalk (**Section F, Deliverable 50**) between infrastructure and applications within 45 days of task order award.

C.6 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The PRS is provided in Section J, Attachment D.